Available online at www.sciencedirect.com
ScienceDirect
European Journal of Combinatorics 29 (2008) 592–600
European Journal of Combinatorics
www.elsevier.com/locate/ejc

Subspaces in d-bounded distance-regular graphs and their applications

Suogang Gao[a], Jun Guo[b], Baohuan Zhang[b], Lihui Fu[c]

[a] *Math. and Inf. College, Hebei Normal University, Shijiazhuang, 050016, China*
[b] *Math. and Inf. College, Langfang Teachers' College, Langfang, 065000, China*
[c] *Dept. of Math., Shijiazhaung Institute of Railway Technology, 050015, China*

Received 7 December 2006; accepted 11 May 2007
Available online 21 May 2007

Abstract

Let Γ be a d-bounded distance-regular graph with diameter $d \geq 3$. For $x \in V(\Gamma)$, let $P(x)$ be the set of all subspaces containing x in Γ. Suppose that $0 \leq t \leq i+t$, $j+t \leq i+j+t \leq d_1 \leq d$, and suppose that Δ and Δ^* are subspaces with diameter $i+t$ and diameter d_1 in $P(x)$, respectively. Let $\Delta \subseteq \Delta^*$; we give the number of subspaces Δ' with diameter $j+t$ and $\Delta' \subseteq \Delta^*$ in $P(x)$ such that $d(\Delta \cap \Delta') = t$ and $d(\Delta + \Delta') = i+j+t$. Using the subspaces in $P(x)$, we construct a new Cartesian authentication code. We also compute its size parameters and its probabilities of successful impersonation attack and of successful substitution attack.

1. Introduction

All graphs considered in this paper are finite undirected graphs without loops or multiple edges. Let $\Gamma = (V(\Gamma), E(\Gamma))$ be a graph with vertex set $V(\Gamma)$ and edge set $E(\Gamma)$. For two vertices $u, v \in V(\Gamma)$, let $\partial_\Gamma(u, v)$ denote the distance between u and v in Γ, i.e., the length of a shortest path connecting u and v. We also write $\partial(u, v)$ when no confusion occurs. Let $d(\Gamma) = \max\{\partial(u, v) \mid u, v \in V(\Gamma)\}$ and call $d(\Gamma)$ the diameter of Γ. We also write $d = d(\Gamma)$ when no confusion occurs. Similarly, the diameter of a subgraph Δ is written as $d(\Delta)$.

For $u \in V(\Gamma)$, set

$$\Gamma_i(u) = \{v \in V(\Gamma) \mid \partial(u, v) = i\}, \qquad \Gamma(u) = \Gamma_1(u).$$

E-mail address: sggao@heinfo.net (S. Gao).

0195-6698/$ - see front matter
doi:10.1016/j.ejc.2007.05.001

For vertices $u, v \in \Gamma$ with $\partial(u, v) = i$, set

$$C(u, v) = C_i(u, v) = \Gamma_{i-1}(u) \cap \Gamma(v),$$
$$A(u, v) = A_i(u, v) = \Gamma_i(u) \cap \Gamma(v),$$
$$B(u, v) = B_i(u, v) = \Gamma_{i+1}(u) \cap \Gamma(v).$$

For the cardinalities of these sets we use lower case letters, i.e.,

$$c_i = c_i(u, v) = |C_i(u, v)|,$$
$$a_i = a_i(u, v) = |A_i(u, v)|,$$
$$b_i = b_i(u, v) = |B_i(u, v)|.$$

A connected graph Γ is said to be *distance-regular* if c_i, a_i, b_i are well defined for all $i, 0 \leq i \leq d(\Gamma)$, i.e., these numbers depend only on i rather than on the individual choice of vertices.

The reader is referred to [1–3,6] for general theory of distance-regular graphs.

For a subset $\Delta \subseteq V(\Gamma)$, we identify Δ with the induced subgraph on Δ and write $\Delta = (V(\Delta), E(\Delta))$.

Recall that a subgraph Δ of Γ is said to be *strongly closed* if $C(u, v) \cup A(u, v) \subseteq \Delta$ for every pair of vertices $u, v \in \Delta$. Properties of strongly closed subgraphs of distance-regular graphs are discussed first by Suzuki in [9]. The term *weak-geodetically closed* is used for strongly closed by Weng in [11]. A *subspace* of Γ is a regular strongly closed subgraph of Γ [11]. It is obvious that the strongly closed subgraphs are connected. If Δ is a strongly closed subgraph of Γ, then for all $u, v \in \Delta$, $\partial_\Gamma(u, v) = \partial_\Delta(u, v)$. We use $\langle\langle x, y \rangle\rangle$ to denote the smallest strongly closed subgraph containing x and y for $x, y \in V(\Gamma)$.

Let Γ be a distance-regular graph with diameter d. Γ is said to be *d-bounded* if the following (i), (ii) hold.

(i) Every strongly closed subgraph of Γ is regular.
(ii) For all $x, y \in V(\Gamma)$, x and y are contained in a common strongly closed subgraph of diameter $\partial(x, y)$.

It is clear that every strongly closed subgraph in d-bounded distance-regular graphs is a subspace.

Let Γ be a d-bounded distance-regular graph with diameter d. Suppose that Δ_1 and Δ_2 are two subspaces in Γ. The intersection of all subspaces that contain Δ_1 and Δ_2 is called the *join* of Δ_1 and Δ_2, and denoted by $\Delta_1 + \Delta_2$.

Now we recall some definitions relevant to authentication codes.

Let $\mathcal{S}$, $\mathcal{E}$ and $\mathcal{M}$ be three non-empty finite sets and let $f : \mathcal{S} \times \mathcal{E} \longrightarrow \mathcal{M}$ be a map. The 4-tuple $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$ is called an *authentication code* [7,8,10] if:

(i) The map $f : \mathcal{S} \times \mathcal{E} \longrightarrow \mathcal{M}$ is surjective.
(ii) Given any $m \in \mathcal{M}$ and $e \in \mathcal{E}$ such that there is an $s \in \mathcal{S}$ satisfying $f(s, e) = m$, then such an s is uniquely determined by the given m and e.

Suppose that $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$ is an authentication code. Then $\mathcal{S}$, $\mathcal{E}$ and $\mathcal{M}$ are called the set of *source states*, the set of *encoding rules*, and the set of *messages*, respectively, and f is called the encoding map. If $s \in \mathcal{S}$, $e \in \mathcal{E}$ and $m \in \mathcal{M}$ are such that $m = f(s, e)$, then we say that the source state s is encoded into the message m under the encoding rule e, and for convenience we say that the massage m contains the encoding rule e. The cardinals $|\mathcal{S}|$, $|\mathcal{E}|$ and $|\mathcal{M}|$ are called the *size*

parameters of the code. Moreover, if the authentication code satisfies the further requirement that given any message m there is a unique source state s such that $m = f(s, e)$ for any encoding rule contained in m, then the code is called a *Cartesian* authentication code.

Authentication codes are used in communication channels where besides the transmitter and the receiver there is an opponent who may play either the impersonation attack or the substitution attack. By an *impersonation attack* we mean that the opponent sends a message through the channel to the receiver and hopes the receiver will accept it as authentic, i.e., as a message sent by the transmitter. By a *substitution attack* we mean that after the opponent intercepts a message sent by the transmitter to the receiver, he/she sends another message instead and hopes the receiver will accept it as authentic. To protect against these attacks the transmitter–receiver may use an authentication code which is publicly known and choose a fixed encoding rule e in secret. The set of information which the transmitter would like to be able to transmit to the receiver should be identified with the set of source states of the code. Suppose that the transmitter wants to send a source state s to the receiver. He/she first encodes s into a message m using the encoding rule e, i.e., $m = f(s, e)$, and then sends m to the receiver. Once the receiver receives a message m', he/she first has to judge whether m' is authentic, i.e., whether the encoding rule e is contained in m'. If e is contained in m', then he/she regards m' as authentic and decodes m' by e to get a source state s', where $m' = f(s', e)$. If e is not contained in m', then he/she regards m' as a false message. The object of the opponent is to choose a message and send it to the receiver so that the probability of deceiving the receiver is as large as possible. We denote by P_I and P_S, respectively, the largest probabilities that he/she could deceive the receiver when he/she plays an impersonation attack and a substitution attack and call them the probabilities of a successful impersonation attack and of a successful substitution attack, respectively.

It is known [4] that in a Cartesian authentication code $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$, $P_I \geq |\mathcal{S}|/|\mathcal{M}|$ and $P_S \geq |\mathcal{S}|/|\mathcal{M}|$. If $P_I = |\mathcal{S}|/|\mathcal{M}|$, we say that P_I is *optimal*, and if $P_S = |\mathcal{S}|/|\mathcal{M}|$, we say that P_S is *optimal*. If both P_I and P_S are optimal, we say that this Cartesian authentication code is *optimal*.

Let Γ be a d-bounded distance-regular graph with diameter $d \geq 3$. Let $x \in V(\Gamma)$ and let $P(x)$ be the set of all subspaces containing x in Γ. The following are our main results.

Theorem 1.1. *Let Γ be a d-bounded distance-regular graph with diameter $d \geq 3$. Suppose that $0 \leq t \leq i+t$, $j+t \leq i+j+t \leq d_1 \leq d$, and suppose that Δ and Δ^* are subspaces with diameter $i+t$ and diameter d_1 in $P(x)$, respectively. Suppose $\Delta \subseteq \Delta^*$. Then the number of subspaces Δ' with diameter $j+t$ and $\Delta' \subseteq \Delta^*$ in $P(x)$ such that $d(\Delta \cap \Delta') = t$ and $d(\Delta + \Delta') = i+j+t$, denoted by $M(t, i+t, j+t; d_1)$, is determined by i, j, t and d_1, independent of the choices of Δ, Δ^*; it is*

$$\frac{(b_0 - b_{i+t})(b_1 - b_{i+t}) \cdots (b_{t-1} - b_{i+t})(b_{i+t} - b_{d_1})(b_{i+t+1} - b_{d_1}) \cdots (b_{i+j+t-1} - b_{d_1})}{(b_0 - b_t)(b_1 - b_t) \cdots (b_{t-1} - b_t)(b_t - b_{j+t})(b_{t+1} - b_{j+t}) \cdots (b_{j+t-1} - b_{j+t})}.$$

Theorem 1.2. *Let Γ be a d-bounded distance-regular graph with diameter $d \geq 3$. Assume that $1 < m_0 < d$, $1 \leq m_1 \leq d - m_0$ and assume that Δ_0 is a fixed subspace with diameter m_0 in $P(x)$. Define the source states to be the subspaces with diameter 1 containing $\{x\}$ and contained in Δ_0. Define the encoding rules to be the subspaces Δ with diameter m_1 such that $\Delta_0 \cap \Delta = \{x\}$ and $d(\Delta_0 + \Delta) = m_0 + m_1$. Define the messages to be the subspaces Δ_2 with diameter $1 + m_1$ in $P(x)$ such that $d(\Delta_0 \cap \Delta_2) = 1$ and $d(\Delta_0 + \Delta_2) = m_0 + m_1$. Denote the set of source states, the set of encoding rules, and the set messages by $\mathcal{S}$, $\mathcal{E}$ and $\mathcal{M}$, respectively. Given any $\Delta \in \mathcal{S}$ and any $\Delta_1 \in \mathcal{E}$, we have that the join $\Delta + \Delta_1$ is a message into which the source state Δ is encoded*

under the encoding rule Δ_1, and that the construction above yields an Cartesian authentication code, whose size parameters are

$$|\mathcal{S}| = \frac{b_0 - b_{m_0}}{b_0 - b_1},$$
$$|\mathcal{E}| = \frac{b_{m_0} b_{m_0+1} \cdots b_{m_0+m_1-1}}{(b_0 - b_{m_1})(b_1 - b_{m_1}) \cdots (b_{m_1-1} - b_{m_1})},$$
$$|\mathcal{M}| = \frac{(b_0 - b_{m_0}) b_{m_0} b_{m_0+1} \cdots b_{m_0+m_1-1}}{(b_0 - b_1)(b_1 - b_{1+m_1})(b_2 - b_{1+m_1}) \cdots (b_{m_1} - b_{1+m_1})}.$$

Assume that the encoding rules are chosen according to a uniform probability distribution. Then its probabilities of successful impersonation attack and of successful substitution attack are

$$P_I = \frac{(b_1 - b_{1+m_1})(b_2 - b_{1+m_1}) \cdots (b_{m_1} - b_{1+m_1})}{b_{m_0} b_{m_0+1} \cdots b_{m_0+m_1-1}},$$
$$P_S = \frac{(b_0 - b_{m_1})(b_1 - b_{m_1}) \cdots (b_{m_1-1} - b_{m_1})}{(b_1 - b_{1+m_1})(b_2 - b_{1+m_1}) \cdots (b_{m_1} - b_{1+m_1})},$$

respectively. Moreover, P_I is optimal.

2. Proof of Theorem 1.1

Proposition 2.1 (*[11] Lemmas 4.2, 4.5*). *Let $\Gamma = (V(\Gamma), E(\Gamma))$ be a d-bounded distance-regular graph with diameter d. Then the following* (i)–(iii) *hold:*

(i) *The intersection of two subspaces is either a subspace or the empty set.*
(ii) *Let Δ be a subspace of Γ and $0 \le i \le d(\Delta)$. Then Δ is distance-regular with intersection numbers $c_i(\Delta) = c_i$, $a_i(\Delta) = a_i$, $b_i(\Delta) = b_i - b_{d(\Delta)}$.*
(iii) *For any $x, y \in V(\Gamma)$, the subspace of diameter $\partial(x, y)$ containing x, y is unique.*

Proposition 2.2 (*[12] Lemma 2.6*). *Let $\Gamma = (V(\Gamma), E(\Gamma))$ be a d-bounded distance-regular graph with diameter d. Then we have $b_i > b_{i+1}$, where $0 \le i \le d-1$.*

Proposition 2.3 (*[5]*). *Let Γ be a d-bounded distance-regular graph with diameter d. Suppose Δ and Δ' are the subspaces with diameter $i+s$ and $i+1$, respectively, where $0 \le i \le i+s \le i+s+1 \le d$. If $d(\Delta \cap \Delta') = i$, then $d(\Delta) + d(\Delta') = d(\Delta \cap \Delta') + d(\Delta + \Delta')$.*

Proposition 2.4 (*[5]*). *Let Γ be a d-bounded distance-regular graph with diameter d. Suppose Δ and Δ' are the subspaces with diameter $i+s$ and $i+t$, respectively, where $0 \le i \le i+s, i+t \le i+s+t \le d$. If $d(\Delta \cap \Delta') = i$, then $d(\Delta) + d(\Delta') \ge d(\Delta \cap \Delta') + d(\Delta + \Delta')$.*

Proposition 2.5 (*[5]*). *Let Γ be a d-bounded distance-regular graph with diameter $d \ge 2$. For $0 \le i, j, t \le d$ and $i+1 \le i+s \le i+s+t \le d$, suppose Δ and Δ' are strongly closed subgraphs with diameter i and $i+s+t$, respectively, and with $\Delta \subseteq \Delta'$. Then the number of the strongly closed subgraphs $\widetilde{\Delta}$ with diameter $i+s$ satisfying $\Delta \subseteq \widetilde{\Delta} \subseteq \Delta'$, denoted by $N(i, i+s; i+s+t)$, is determined by i, s and t, independent of the choice of Δ and Δ'; it is*

$$\frac{(b_i - b_{i+s+t})(b_{i+1} - b_{i+s+t}) \cdots (b_{i+s-1} - b_{i+s+t})}{(b_i - b_{i+s})(b_{i+1} - b_{i+s}) \cdots (b_{i+s-1} - b_{i+s})}.$$

Lemma 2.6. *Let Γ be a d-bounded distance-regular graph with diameter $d \geq 2$. Suppose that Δ and Δ' are two subspaces in Γ with $\Delta \subseteq \Delta'$, and suppose that there exists $x \in \Delta$ such that x has the same valency in Δ and Δ'. Then $\Delta = \Delta'$.*

Proof. Set $d(\Delta) = d_1$ and $d(\Delta') = d_2$. By Proposition 2.1(ii), we obtain that both Δ and Δ' are distance-regular and $k(\Delta) = b_0 - b_{d_1}$, $k(\Delta') = b_0 - b_{d_2}$. Since x has the same valency in Δ and Δ', $k(\Delta) = k(\Delta')$. It follows that $b_{d_1} = b_{d_2}$. By Proposition 2.2, we have $d_1 = d_2$. It follows from Proposition 2.1(iii) that $\Delta = \Delta'$. □

Lemma 2.7. *Let Γ be a d-bounded distance-regular graph with diameter $d \geq 2$. Suppose that Δ and Δ' are two subspaces in Γ, and suppose that*

$$j = \max\{\partial(x, y) \mid x \in \Delta, y \in \Delta'\}.$$

Then $\Delta + \Delta'$ is the unique subspace with diameter j containing Δ and Δ'.

Proof. Suppose that $x \in \Delta$ and $y \in \Delta'$ are such that $\partial(x, y) = j$. Then $\langle\langle x, y\rangle\rangle$ is a subspace with diameter j. Since $x \in \Delta \cap \langle\langle x, y\rangle\rangle$, we have $\Delta \cap \langle\langle x, y\rangle\rangle \neq \emptyset$. It follows from Proposition 2.1 that $\Delta \cap \langle\langle x, y\rangle\rangle$ is also a subspace. Assume that u is a vertex in Δ adjacent to x. Then $\partial(u, y) = j - 1$ or j. By the definition of a subspace, we obtain $u \in C(y, x) \cup A(y, x) \subseteq \langle\langle x, y\rangle\rangle$. This implies that all the vertices adjacent to x in Δ are in $\langle\langle x, y\rangle\rangle$. Thus, x has the same valency in $\Delta \cap \langle\langle x, y\rangle\rangle$ and Δ. It follows from Lemma 2.6 that $\Delta \cap \langle\langle x, y\rangle\rangle = \Delta$, which implies that $\Delta \subseteq \langle\langle x, y\rangle\rangle$. Similarly, we have $\Delta' \subseteq \langle\langle x, y\rangle\rangle$. So $\Delta + \Delta' = \langle\langle x, y\rangle\rangle$, and hence $\Delta + \Delta'$ is the unique subspace with diameter j containing Δ and Δ'. □

Lemma 2.8. *Let Γ be a d-bounded distance-regular graph with diameter $d \geq 2$. For $0 \leq i \leq i + s, i + t \leq i + s + t \leq d$, let Δ and Δ' be two subspaces in Γ with diameters $i + s$ and $i + t$, respectively, such that $d(\Delta \cap \Delta') = i$. If*

$$d(\Delta) + d(\Delta') = d(\Delta \cap \Delta') + d(\Delta + \Delta'),$$

then the following hold:

(i) *For fixed $x, y \in \Delta \cap \Delta'$ with $\partial(x, y) = i$, for all vertices $u \in \Delta$ with $\partial(u, x) = l$, $\partial(u, y) = i + l$, $0 \leq l \leq s$, and for all vertices $v \in \Delta'$ with $\partial(x, v) = i + m$, $\partial(y, v) = m$, $0 \leq m \leq t$, we have $\partial(u, v) = i + l + m$.*

(ii) *For all subspaces Δ_1 containing $\Delta \cap \Delta'$ in Δ, and for all subspaces Δ_2 containing $\Delta \cap \Delta'$ in Δ', we have*

$$d(\Delta_1) + d(\Delta_2) = d(\Delta_1 \cap \Delta_2) + d(\Delta_1 + \Delta_2).$$

Proof. (i) Clearly, $\langle\langle x, y\rangle\rangle = \Delta \cap \Delta'$ by Proposition 2.1. Suppose that $\partial(u, x) = l$ and $\partial(u, y) = i + l$, where $u \in \Delta, 0 \leq l \leq s$. Then we can choose a sequence of vertices in Δ, $u = u_l, u_{l+1}, \ldots, u_s$, such that $u_p \in B(y, u_{p-1})$, where $l + 1 \leq p \leq s$. It follows from Proposition 2.1 that $\Delta = \langle\langle u_s, y\rangle\rangle$. Suppose that $\partial(x, v) = i + m$ and $\partial(y, v) = m$, where $v \in \Delta', 0 \leq m \leq t$. We will show that $\partial(u_s, v) = i + s + m$ by induction for m. The conclusion is clearly true for $m = 0$. Suppose that $m \geq 1$, and suppose that the conclusion is true for $m - 1$. Then there exists a vertex $v_1 \in \Delta'$ such that $\partial(v_1, v) = 1$, $\partial(x, v_1) = i + m - 1$ and $\partial(y, v_1) = m - 1$. By induction, $\partial(u_s, v_1) = i + s + m - 1$. It follows that $i + s + m - 2 \leq \partial(u_s, v) \leq i + s + m$. If $i + s + m - 2 \leq \partial(u_s, v) \leq i + s + m - 1$, then $v \in C(u_s, v_1) \cup A(u_s, v_1) \subseteq \langle\langle u_s, v_1\rangle\rangle$ since

$\langle\langle u_s, v_1\rangle\rangle$ is a subspace. Note that $\Delta \subseteq \langle\langle u_s, v_1\rangle\rangle$, so $\Delta + \Delta' \subseteq \langle\langle u_s, v_1\rangle\rangle + \Delta'$. It follows from Proposition 2.4 that

$$\begin{aligned} i + s + t &= d(\Delta + \Delta') \le d(\langle\langle u_s, v_1\rangle\rangle + \Delta') \\ &\le d(\langle\langle u_s, v_1\rangle\rangle) + d(\Delta') - d(\langle\langle u_s, v_1\rangle\rangle \cap \Delta') \\ &= (i + s + m - 1) + (i + t) - d(\langle\langle u_s, v_1\rangle\rangle \cap \Delta'). \end{aligned}$$

This implies that $d(\langle\langle u_s, v_1\rangle\rangle \cap \Delta') \le i + m - 1$. Note that $x \in \langle\langle u_s, v_1\rangle\rangle \cap \Delta'$, so $\langle\langle x, v_1\rangle\rangle \subseteq \langle\langle u_s, v_1\rangle\rangle \cap \Delta'$. By Proposition 2.1, we have $\langle\langle x, v_1\rangle\rangle = \langle\langle u_s, v_1\rangle\rangle \cap \Delta'$. So $v \in \langle\langle u_s, v_1\rangle\rangle \cap \Delta' = \langle\langle x, v_1\rangle\rangle$, contradicting the fact that the diameter of $\langle\langle x, v_1\rangle\rangle$ is $i + m - 1$. So $\partial(u_s, v) = i + s + m$. From the argument above we have proved that the result is true for m, and for all m by the principle of induction. The assertion (i) is proved.

(ii) Let $x, y \in \Delta \cap \Delta'$ with $\partial(x, y) = i$. Then $\langle\langle x, y\rangle\rangle = \Delta \cap \Delta'$ by Proposition 2.1. For all subspaces Δ_1 with diameter $i + l$, where $0 \le l \le s$, containing $\Delta \cap \Delta'$ in Δ, we have that there exists a vertex $u \in \Delta_1$ such that $\partial(u, x) = l$ and $\partial(u, y) = i + l$. Similarly, for all subspaces Δ_2 with diameter $i + m$, $0 \le m \le t$, containing $\Delta \cap \Delta'$ in Δ', we have that there exists a vertex $v \in \Delta_2$ such that $\partial(y, v) = m$, $\partial(x, v) = i + m$. By Proposition 2.1(iii), we obtain

$$\Delta_1 = \langle\langle u, y\rangle\rangle, \qquad \Delta_2 = \langle\langle x, v\rangle\rangle.$$

By the argument of (i), $\partial(u, v) = i + l + m$. Since $\Delta_1 \subseteq \langle\langle u, v\rangle\rangle$ and $\Delta_2 \subseteq \langle\langle u, v\rangle\rangle$, $\Delta_1 + \Delta_2 \subseteq \langle\langle u, v\rangle\rangle$. Note that $\langle\langle u, v\rangle\rangle \subseteq \Delta_1 + \Delta_2$, so $\Delta_1 + \Delta_2 = \langle\langle u, v\rangle\rangle$. Since $\Delta_1 \cap \Delta_2 = \Delta \cap \Delta'$,

$$d(\Delta_1) + d(\Delta_2) = d(\Delta_1 \cap \Delta_2) + d(\Delta_1 + \Delta_2). \quad \square$$

Proof of Theorem 1.1. We divide the proof into three steps.

Step 1. Let $\widetilde{\Delta}$ be a subspace in Δ^* with diameter $i + j + t$ containing Δ. Since $d(\Delta) = i + t$, there exist $x, y, z \in \Delta$ such that $\partial(x, y) = i$, $\partial(x, z) = t$ and $\partial(y, z) = i + t$. It follows from Proposition 2.1(iii) that $\Delta = \langle\langle y, z\rangle\rangle$. In the following, for each $\langle\langle x, z\rangle\rangle \subseteq \Delta$, we will compute the number of Δ' in $\widetilde{\Delta}$ with diameter $j + t$ such that $\Delta \cap \Delta' = \langle\langle x, z\rangle\rangle$ and $\Delta + \Delta' = \widetilde{\Delta}$.

First, choose the sequences of vertices in $\widetilde{\Delta}$, $z = u_0, u_1, \ldots, u_j = w$, such that $u_l \in B(y, u_{l-1}) \cap \widetilde{\Delta}$, where $1 \le l \le j$. From Proposition 2.1(iii), we have that $\widetilde{\Delta} = \langle\langle y, w\rangle\rangle$ and that $\Delta' = \langle\langle x, w\rangle\rangle$ is a subspace with diameter $j + t$. Clearly, $d(\Delta + \Delta') = d(\widetilde{\Delta})$. It follows from Proposition 2.4 that

$$i + j + t = d(\Delta + \Delta') \le d(\Delta) + d(\Delta') - d(\Delta \cap \Delta').$$

This implies that $d(\Delta \cap \Delta') \le t$. By Proposition 2.1(iii), $\Delta \cap \Delta' = \langle\langle x, z\rangle\rangle$. Thus Δ' is a subspace such that $\Delta \cap \Delta' = \langle\langle x, z\rangle\rangle$. Since the number of choices of the above vertex sequences in $\widetilde{\Delta}$ is

$$e = (b_{i+t} - b_{i+j+t})(b_{i+t+1} - b_{i+j+t}) \cdots (b_{i+t+j-1} - b_{i+j+t}),$$

the number of Δ' in $\widetilde{\Delta}$ with diameter $j + t$ such that $\Delta \cap \Delta' = \langle\langle x, z\rangle\rangle$ and $\Delta + \Delta' = \widetilde{\Delta}$ is e.

Next, we will consider the number of times that every Δ' repeats. For any such Δ', choose a sequence of vertices in Δ', $z = v_0, v_1, \ldots, v_j = w$, such that $v_l \in B(x, v_{l-1}) \cap \Delta'$, $1 \le l \le j$. By Lemma 2.8, we have $\partial(y, v_j) = i + j + t$, and hence $\langle\langle y, v_j\rangle\rangle = \widetilde{\Delta}$. From Proposition 2.1(ii), there are in total

$$e' = (b_t - b_{j+t})(b_{t+1} - b_{j+t}) \cdots (b_{j+t-1} - b_{j+t})$$

such sequences of vertices in Δ'. So the number of times that every Δ' repeats is e'.

Finally, let Δ' be a subspace with diameter $j+t$ in $\widetilde{\Delta}$ such that $\Delta \cap \Delta' = \langle\langle x, z\rangle\rangle$ and $\Delta + \Delta' = \widetilde{\Delta}$; we will prove Δ' must be one of the above e/e' subspaces. Set

$$h = \max\{\partial(y, w) \mid w \in \Delta'\}.$$

Then there exists a vertex u in Δ' such that $\partial(y, u) = h$. By Lemma 2.7, there exists a unique subspace, say Δ^1, with diameter h containing $\{y\}$ and Δ'. Since $\langle\langle x, z\rangle\rangle \subseteq \Delta' \subseteq \Delta^1$, $\Delta = \langle\langle y, z\rangle\rangle \subseteq \Delta^1$. This implies that Δ^1 is a subspace containing Δ and Δ'. Note that

$$\Delta^1 = \langle\langle y, u\rangle\rangle \subseteq \Delta + \Delta' = \widetilde{\Delta},$$

so $\Delta^1 = \widetilde{\Delta}$, and hence $h = i+j+t$. Since $\partial(y, x)+\partial(x, u) \geq \partial(y, u) = i+j+t$, $\partial(x, u) \geq j+t$. Note that $d(\Delta') = j+t$, so $\Delta' = \langle\langle x, u\rangle\rangle$. Choose a vertex v in Δ' such that $\partial(z, v) = j$ and $\partial(x, v) = j+t$. Then $\Delta' = \langle\langle x, v\rangle\rangle$. By Lemma 2.8, we have $\partial(y, v) = i+j+t$, and hence $\widetilde{\Delta} = \langle\langle y, v\rangle\rangle$. This implies that Δ' must be one of the above e/e' subspaces. Thus the number of Δ' in $\widetilde{\Delta}$ with diameter $j+t$ such that $\Delta \cap \Delta' = \langle\langle x, z\rangle\rangle$ and $\Delta + \Delta' = \widetilde{\Delta}$ is e/e'.

Step 2. By Proposition 2.5, there are $N(0, t; i+t)$ subspaces with diameter t containing $\{x\}$ in Δ. It follows from Proposition 2.1(iii) that the number of subspaces Δ' in $\widetilde{\Delta}$ with diameter $j+t$ containing $\{x\}$ such that $d(\Delta \cap \Delta') = t$ and $\Delta + \Delta' = \widetilde{\Delta}$ is $N(0, t; i+t)e/e'$.

Step 3. Let $\widetilde{\Delta}$ and $\widetilde{\Delta}_1$ be two different subspaces in $P(x)$ with diameter $i+j+t$ containing Δ. Suppose that Δ' is a subspace in $\widetilde{\Delta}$ with diameter $j+t$ containing $\{x\}$ such that $d(\Delta \cap \Delta') = t$ and $\Delta + \Delta' = \widetilde{\Delta}$. Also suppose that Δ'_1 is a subspace in $\widetilde{\Delta}_1$ with diameter $j+t$ containing $\{x\}$ such that $d(\Delta \cap \Delta'_1) = t$ and $\Delta + \Delta'_1 = \widetilde{\Delta}_1$. We claim that $\Delta' \neq \Delta'_1$. Suppose not. Then $\Delta + \Delta' = \Delta + \Delta'_1$. By $d(\widetilde{\Delta}) = i+j+t = d(\widetilde{\Delta}_1)$ and Proposition 2.1(iii), $\widetilde{\Delta} = \widetilde{\Delta}_1$, a contradiction. From Proposition 2.5, there are $N(i+t, i+j+t; d_1)$ subspaces $\widetilde{\Delta}$ in Δ^* with diameter $i+j+t$ containing Δ. Hence the number of subspaces Δ' in Δ^* with diameter $j+t$ such that $d(\Delta \cap \Delta') = t$ and $d(\Delta + \Delta') = i+j+t$ is $N(i+t, i+j+t; d_1)N(0, t; i+t)e/e'$. From Proposition 2.5, we have the desired result. □

3. Proof of Theorem 1.2

Lemma 3.1. *The construction in Theorem 1.2 yields a Cartesian authentication code.*

Proof. Let Δ be a source state and Δ_1 be an encoding rule. Since $\Delta \subseteq \Delta_0$, $\{x\} \subseteq \Delta \cap \Delta_1 \subseteq \Delta_0 \cap \Delta_1 = \{x\}$. This implies that $\Delta \cap \Delta_1 = \{x\}$. It follows from Proposition 2.3 that $d(\Delta+\Delta_1) = d(\Delta) + d(\Delta_1) - d(\Delta \cap \Delta_1) = 1 + m_1$. By Proposition 2.4 and $(\Delta + \Delta_1) + \Delta_0 = \Delta_1 + \Delta_0$, $d((\Delta + \Delta_1) \cap \Delta_0) \leq 1 + m_1 + m_0 - (m_0 + m_1) = 1$. It follows from $\Delta \subseteq (\Delta + \Delta_1) \cap \Delta_0$ and Proposition 2.1(iii) that $(\Delta + \Delta_1) \cap \Delta_0 = \Delta$. This implies that $\Delta + \Delta_1$ is a message.

Next, let Δ_2 be a message. Set $\Delta = \Delta_0 \cap \Delta_2$. Then Δ is a source state. Suppose that Δ_1 is a subspace with diameter m_1 contained in Δ_2 such that $\Delta \cap \Delta_1 = \{x\}$. Then $\Delta_1 \cap \Delta_0 \subseteq \Delta_2 \cap \Delta_0 = \Delta$. Since $\Delta_1 \cap \Delta_0 \subseteq \Delta_1$, $\Delta_1 \cap \Delta_0 \subseteq \Delta \cap \Delta_1 = \{x\}$, and hence $\Delta_1 \cap \Delta_0 = \{x\}$. This implies that Δ_1 is an encoding rule.

Suppose now that there is another source state Δ' which is encoded into message Δ_2. Then $\Delta' \subseteq \Delta_0$ and $\Delta' \subseteq \Delta_2$. Thus $\Delta' \subseteq \Delta_0 \cap \Delta_2 = \Delta$. By Proposition 2.1(iii), we deduce $\Delta = \Delta'$. This proves that the source state Δ is uniquely determined by Δ_2. □

Lemma 3.2.

$$|\mathcal{S}| = N(0, 1; m_0) = \frac{b_0 - b_{m_0}}{b_0 - b_1},$$

$$|\mathcal{E}| = M(0, m_0, m_1; d) = \frac{b_{m_0} b_{m_0+1} \cdots b_{m_0+m_1-1}}{(b_0 - b_{m_1})(b_1 - b_{m_1}) \cdots (b_{m_1-1} - b_{m_1})},$$

$$|\mathcal{M}| = M(1, m_0, 1+m_1; d) = \frac{(b_0 - b_{m_0}) b_{m_0} b_{m_0+1} \cdots b_{m_0+m_1-1}}{(b_0 - b_1)(b_1 - b_{1+m_1})(b_2 - b_{1+m_1}) \cdots (b_{m_1} - b_{1+m_1})}.$$

Proof. It is clear by the construction, Proposition 2.5 and Theorem 1.1. □

Lemma 3.3. *The number of encoding rules contained in a message is*

$$\frac{(b_1 - b_{1+m_1})(b_2 - b_{1+m_1}) \cdots (b_{m_1} - b_{1+m_1})}{(b_0 - b_{m_1})(b_1 - b_{m_1}) \cdots (b_{m_1-1} - b_{m_1})}.$$

Proof. Let Δ_2 be a message and let $\Delta = \Delta_2 \cap \Delta_0$ be the unique source state contained in Δ_2. Then we claim that the encoding rules contained in Δ_2 coincide with the subspaces Δ_1 with diameter m_1 in Δ_2 such that $\Delta \cap \Delta_1 = \{x\}$ and $\Delta + \Delta_1 = \Delta_2$. Indeed, let Δ_1 be an encoding rule contained in Δ_2. By the construction, Δ_1 is the subspace such that $\Delta_0 \cap \Delta_1 = \{x\}$ and $d(\Delta_0 + \Delta_1) = m_0 + m_1$. By Lemma 2.8, Δ is the subspace with m_1 in Δ_2 such that $\Delta \cap \Delta_1 = \{x\}$ and $\Delta + \Delta_1 = \Delta_2$. Conversely, let Δ be the subspace with diameter m_1 in Δ_2 such that $\Delta \cap \Delta_1 = \{x\}$ and $\Delta + \Delta_1 = \Delta_2$. Since

$$\Delta_1 \cap \Delta_0 \subseteq \Delta_2 \cap \Delta_0 = \Delta,$$

we have

$$\Delta_1 \cap \Delta_0 \subseteq \Delta \cap \Delta_1 = \{x\}.$$

Note that

$$\Delta \subseteq \Delta_0 \cap (\Delta + \Delta_1) \subseteq \Delta_0 \cap \Delta_2 = \Delta,$$

so $\Delta_0 \cap (\Delta + \Delta_1) = \Delta$. Thus,

$$d(\Delta_0 + (\Delta + \Delta_1)) = m_0 + m_1 = d(\Delta_0 + \Delta_1),$$

and hence Δ_1 is the encoding rule contained in Δ_2.

Therefore, by Theorem 1.1, the number of encoding rules contained in a message is

$$\frac{(b_1 - b_{1+m_1})(b_2 - b_{1+m_1}) \cdots (b_{m_1} - b_{1+m_1})}{(b_0 - b_{m_1})(b_1 - b_{m_1}) \cdots (b_{m_1-1} - b_{m_1})}. \quad \square$$

Lemma 3.4. *Let Δ_2 and Δ_2' be two different massages which contain an encoding rule in common and let Δ, Δ' be the unique source states contained in Δ_2 and Δ_2', respectively. Then $\Delta \cap \Delta' = \{x\}$ and the number of encoding rules contained in both Δ_2 and Δ_2' is* 1.

Proof. Clearly, $\Delta = \Delta_2 \cap \Delta_0$ and $\Delta' = \Delta_2' \cap \Delta_0$. Write $d_1 = d(\Delta_2 \cap \Delta_2')$. Since Δ_2 and Δ_2' have an encoding rule in common, $d_1 = m_1$. Write $\Delta_3 = \Delta \cap \Delta'$. Then $d(\Delta_3) = 0$. Thus the number of encoding rules contained in both Δ_2 and Δ_2' is 1. □

Lemma 3.5. *Assume that the encoding rules are chosen according to a uniform probability distribution, and denote the probabilities of a successful impersonation attack and of a successful*

substitution attack by P_I and P_S, respectively. Then

$$P_I = \frac{(b_1 - b_{1+m_1})(b_2 - b_{1+m_1}) \cdots (b_{m_1} - b_{1+m_1})}{b_{m_0} b_{m_0+1} \cdots b_{m_0+m_1-1}},$$

$$P_S = \frac{(b_0 - b_{m_1})(b_1 - b_{m_1}) \cdots (b_{m_1-1} - b_{m_1})}{(b_1 - b_{1+m_1})(b_2 - b_{1+m_1}) \cdots (b_{m_1} - b_{1+m_1})}.$$

Proof. By Lemmas 3.2 and 3.3,

$$P_I = \frac{(b_1 - b_{1+m_1})(b_2 - b_{1+m_1}) \cdots (b_{m_1} - b_{1+m_1})}{(b_0 - b_{m_1})(b_1 - b_{m_1}) \cdots (b_{m_1-1} - b_{m_1})|\mathcal{E}|}.$$

By Lemmas 3.3 and 3.4,

$$P_S = \frac{(b_0 - b_{m_1})(b_1 - b_{m_1}) \cdots (b_{m_1-1} - b_{m_1})}{(b_1 - b_{1+m_1})(b_2 - b_{1+m_1}) \cdots (b_{m_1} - b_{1+m_1})}. \quad \square$$

Proof of Theorem 1.2. It is obvious from Lemmas 3.1–3.5. By $P_I = |\mathcal{S}|/|\mathcal{M}|$, P_I is optimal. $\square$

Acknowledgements

The authors are grateful to the referees for their valuable suggestions. This paper was supported by Natural Science Foundation of Hebei Province, China (No. A2005000141), and Educational Committee of Hebei Province, China (No. 2005107).

References

[1] E. Bannai, T. Ito, Algebraic Combinatorics *I*: Association Schemes, Benjamin-Cummings, California, 1984.
[2] N.L. Biggs, Algebraic Graph Theory, Cambridge University Press, Califonia, 1993.
[3] A.E. Brouwer, A.M. Cohen, A. Neumaier, Distance-Regular Graphs, Springer-Verlag, Berlin, Heidelberg, 1989.
[4] R. Feng, J.H. Kwak, Isomorphism classes of authentication codes, Bull. Aust. Math. Soc. 69 (2004) 203–215.
[5] S. Gao, J. Guo, W. Liu, Lattices generated by strongly closed subgraphs in d-bounded distance-regular graphs, European J. Combin. (in press).
[6] C.D. Godsil, Algebraic Combinatorics, Chapman and Hall, New York, 1993.
[7] G.J. Simmons, Authentication theory/coding theory, in: Advances in Cryptology, Proceedings of Crypto 84, in: Lecture Notes in Computer Science, vol. 196, Springer, 1985, pp. 411–431.
[8] D.R. Stinson, The combinatorics of authentication and secrecy codes, J. Cryptology 2 (1990) 23–49.
[9] H. Suzuki, On strongly closed subgraphs of highly regular graphs, European J. Combin. 16 (1995) 197–220.
[10] Z. Wan, Further construction of Cartesian authentication codes from symplectic geometry, Northeast. Math. J. 8 (1992) 4–20.
[11] C. Weng, Classical distance-regular graphs of negative type, J. Combin. Theory Ser. B 76 (1999) 93–116.
[12] C. Weng, D-bounded distance-regular graphs, European J. Combin. 18 (1997) 211–229.